2020 Statewide Glossary Updates

May 2020

Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
AAM	**Add**	Acronym		After Action Meeting	FEMA
AAR	**Add**	Acronym		After Action Report	FEMA
After Action Meeting (AAM)	**Add**			The AAM is a meeting held among elected and appointed officials or their designees from the exercising organizations, as well as the lead evaluator and members of the exercise planning team, to debrief the exercise and to review and refine the draft AAR/IP. The AAM should be an interactive session, providing attendees the opportunity to discuss and validate the analytical findings and corrective actions in the draft AAR/IP.	FEMA
After Action Report (AAR)	**Add**			A document containing findings and recommendations from an exercise or a test.	NIST
Agency Critical	**Modify**	Renamed term from "Department Critical" and modified definition	From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes and/or activities.	*See* , Application Criticality.	FEMA
All-Hazards	**Modify**		The spectrum of all types of hazards including accidents; technological events; natural disasters; terrorist attacks; warfare; and, chemical, biological (including pandemic influenza), radiological, nuclear, or explosive events.	A classification encompassing all conditions, environmental or human-caused, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects. These include accidents, technological events, natural disasters, space weather, domestic and foreign-sponsored terrorist attacks, acts of war, weapons of mass destruction, and chemical, biological (including pandemic), radiological, nuclear, or explosive events.	FEMA
Alternate Locations	**Modify**	Renamed term from "Alternate Sites" and modified definition	Alternate sites are locations other than the primary facility used to carry out Essential Functions by relocating ERG members following activation of the Continuity Plan. These sites refer to facilities, locations, and also work arrangements such as telework and mobile work concepts.	Fixed, mobile, or transportable locations, other than the primary operating facility, where leadership and continuity personnel relocate in order to perform essential functions following activation of the continuity plan.	FEMA
Application	**Modify**		A computer system (potentially including multiple programs, modules, etc.) designed to accomplish operational tasks or functions that help a user perform his or her work. Applications typically fall into one of four categories: Core Business; Desktop; Common Services & Integration; and Process Automation. It is also a generic term for a program or system that handles a specific business function.	A software program hosted by an information system. This is in contrast to software such as operating systems.	NIST
Application Criticality	**Modify**		Application Criticality – Application criticality has the following categories. • Statewide Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to statewide core functions, processes and/or activities. The applications loss may also impact a large portion of the State's population. • Department Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes and/or activities. • Program Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to the core functions, processes and/or activities associated with a program within an agency. • Non Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have little or no impact to statewide and/or this department's core functions, processes and activities or the core functions, processes and activities associated with a program within an agency.	Application Criticality – Application criticality has the following categories. • Statewide Critical – Based on the agency's analysis, this application has a direct impact to statewide essential functions, processes, activities, or population. • Agency Critical – Based on the agency's analysis, this application has a direct impact to this agency's essential functions, processes and/or activities. • Program Critical – Based on the agency's analysis, this application has a direct impact to the essential functions, processes and/or activities associated with a program within the agency. • Non-Critical – Based on the agency's analysis, this application has no direct impact to a state, agency, or program's essential functions, processes and activities within the agency.	FEMA
Asset	**Add**			Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).	NIST
BPA	**Add**	Acronym		Business Process Analysis	FEMA
Business Impact Analysis (BIA)	**Modify**		A management level analysis, which identifies the impacts of losing organizational information technology resources. A BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.	A method of identifying the consequences of failing to perform a function or requirement.	FEMA
Business Process Analysis (BPA)	**Modify**		A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and facilities inherent in the execution of a function or requirement.	A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and alternate locations inherent in the execution of a function or requirement.	FEMA

2020 Statewide Glossary Updates

May 2020

Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
CIRP	**Add**	Acronym		Cyber Incident Response Plan, *See* , IRP.	NIST
CIRT	**Add**	Acronym		Cyber Incident Response Team	NIST
Cold Site	**Add**			A facility that is neither staffed nor operational on a daily basis. Telecommunications, IT equipment, and infrastructure is typically present at the location, however teams of specialized personnel must be deployed to activate the systems before the site can become operational. Basic infrastructure and environmental controls are present (e.g., electrical and heating, ventilation and air conditioning systems), yet systems are not continuously active.	FEMA
Computer Incident Response Team (CIRT)	**Add**			*See* , Cyber Incident Response Team.	NIST
Continuity	**Modify**		An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event.	The ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an incident that disrupts normal operations	FEMA
Continuity Capability	**Add**			The ability of an organization to continue to perform its essential functions, using COOP and COG programs and continuity requirements that have been integrated into the organization's daily operations. The primary goal is preserving of our form of government under the U.S. Constitution and the continued performance of NEFs and organizational essential functions under all conditions.	FEMA
Continuity Coordinator	**Add**			The senior accountable official, designated by leadership or elected officials, who is responsible for oversight of the continuity program. Continuity coordinators are supported by a continuity manager and other continuity planners within subcomponent levels throughout the organization or government. Also referred to as agency management in the Statewide Information Security Manual (SISM) Contingency Planning policy.	FEMA
Continuity Facilities	**Remove**	Term was removed			FEMA
Continuity of Government (COG)	**Modify**		The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services.	A coordinated effort within the executive, legislative, or judicial branches to ensure that essential functions continue to be performed before, during, and after an emergency or threat. Continuity of government is intended to preserve the statutory and constitutional authority of elected officials at all levels of government across the United States.	FEMA
Continuity of Government Readiness Conditions (COGCON)	**Remove**	Term was removed			FEMA
CSIRP	**Add**	Acronym		Computer Security Incident Response Plan, See, Incident Response Plan	NIST
CSIRT	**Add**	Acronym		Computer Security Incident Response Team, See, Cyber Incident Response Team.	NIST
CTA	**Add**	Acronym		Cyber Threat Actor	
Cyber Incident Response Team (CIRT)	**Add**			Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT).	NIST
Cyber Threat Actor (CTA)	**Add**			An individual or a group posing a cyber threat. This threat can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.	NIST, DHS-CISA
Cybercriminal	**Add**			A cyber threat actor who uses a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.	Encyclopedia Britannica
EAS	**Add**	Acronym		Emergency Alert System	FEMA
EndEx	**Add**	Acronym		End of Exercise	FEMA
End of Exercise (EndEx)	**Add**			The official conclusion of an exercise.	FEMA
Ground Truth	**Add**			The ground truth is comprised of the detailed elements of a prevention exercise scenario that must remain consistent during exercise development and conduct to ensure that realism is maintained and objectives may be met in the unscripted move-countermove exercise environment. The ground truth includes the scenario timeline, local threat environment, simulated threat group, and individual adversary profiles and relationships. Once composed, the ground truth is used as the basis for Master Scenario Events List (MSEL) development and red team operations planning, if applicable.	FEMA
Hacktivism	**Add**			Computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism.	Merriam-Webster

2020 Statewide Glossary Updates

May 2020

Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
Host on Demand (HOD)	**Add**			HOD is a terminal emulator that provides browser-based or non-browser-based client access to IBM mainframe resources.	IBM
Hot Wash	**Add**			A “Hot Wash” is a post-action review completed within 24 hours of an incident or exercise (or as soon as practical). It is imperative that this review is kept positive in tone; finger-pointing is not constructive and will prevent the honest dialog required for improvement.	FEMA
Improvement Plan	**Add**			The improvement plan identifies specific corrective actions, assigns them to responsible parties, and establishes target dates for their completion. The improvement plan is developed in conjunction with the After-Action Report.	FEMA
Incident Response Plan	**Add**			The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization’s information systems(s).	NIST
Insider Threat	**Add**			An entity with authorized access that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.	NIST
IRP	**Add**	Acronym		Incident Response Plan	NIST
MSEL	**Add**	Acronym		Master Scenario Events List	FEMA
Master Scenario Events List (MSEL)	**Add**			The MSEL is a chronological timeline of expected actions and scripted events to be injected into exercise play by controllers to generate or prompt player activity. It ensures necessary events happen so that all objectives are met. Larger, more complex exercises may also use a procedural flow, which differs from the MSEL in that it contains only expected player actions or events. The MSEL links simulation to action, enhances exercise experience for players, and reflects an incident or activity meant to prompt players to action.	FEMA
Nation-State Threat Actor	**Modify**	Renamed term from "Nation State" and modified definition	A nation state threat actor is a type of Advanced Persistent Threat (APT). The nation state threat actor receives direction and support from an established nation state (government). The line between nation-state cyber activity and cybercrime is often blurred as organized crime groups are afforded a degree of support.	National cyber warfare programs that pose threats that range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption	DHS-CISA
Non-Critical	**Modify**		In the agency’s opinion, the loss of an application will have little or no impact to Statewide and/or agency core functions, processes and activities or the core functions, processes and activities associated with a program within the agency.	*See* , Application Criticality or Process Criticality.	FEMA
Preparedness	**Add**			The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of an agency, state, and the nation.	FEMA
Privileged Account	**Modify**		An account of an information system that has more authority and access than a normal user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router access.	An account of an information system that has elevated or special access or more authority than a normal user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router access.	NC DIT
Process Criticality	**Add**			Process Criticality – Process criticality has the following categories. • Statewide Critical – Based on the agency’s analysis, this process has a direct impact to statewide essential functions, processes, activities or population. • Agency Critical – Based on the agency’s analysis, this process has a direct impact to the agency’s essential functions, processes and/or activities. • Program Critical – Based on the agency’s analysis, this process has a direct impact to the essential functions, processes and/or activities associated with a program within the agency. • Non-Critical – Based on the agency’s analysis, this process has no direct impact to a state, agency, or program’s essential functions, processes and activities within the agency.	FEMA
Program Critical	**Modify**		From an information technology perspective, in the agency’s opinion, the loss of this application will have a direct impact to the core functions, processes and/or activities associated with a program within this agency.	*See* , Application Criticality.	FEMA

2020 Statewide Glossary Updates

May 2020

Term	Action	Description/Notes	Current Definition	New Term/Definition	Source
Public Records	**Modify**		All documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.	As defined by N.C.G.S 132-1, all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.	NC DIT
RCA	**Add**	Acronym		Root-Cause Analysis	FEMA
Request for Proposal (RFP)	**Modify**		Formal statement by a department that it is soliciting enterprises to bid on a contract for a program, system or service.	Formal statement by an organization that it is soliciting vendors to bid on a contract for a program, system or service.	NC DIT
Root-Cause Analysis (RCA)	**Add**			When evaluating exercises, root-cause analysis involves not merely identifying what issues emerged, but rather discovering the root causes of those issues. Root-cause analysis enables exercise stakeholders to target how best to address areas for improvement and close capability gaps.	FEMA
Separation of Duties	**Modify**		The use of more than one individual to handle a particular (generally important) activity.	The use of more than one individual to handle a particular (generally important) activity to distribute the associated privilege of authority among multiple individuals or entities. The goal is to eliminate the possibility of a single user or entity from carrying out and concealing a prohibited action.	OWASP
SISM	**Add**	Acronym		Statewide Information Security Manual	
SME	**Add**	Acronym		Subject Matter Expert	FEMA
StartEx	**Add**	Acronym		Start of Exercise	FEMA
Start of Exercise (StartEx)	**Add**			The official beginning of an exercise.	FEMA
Subject-Matter Expert (SME)	**Add**			SMEs have functional knowledge and expertise in a specific area or in performing a specialized job, task, or skill. As part of an exercise planning team, they help make the scenario realistic and plausible and ensure agencies and/or the state has the appropriate capabilities to respond. SMEs are ideal for the positions of controllers and evaluators.	FEMA
Tabletop Exercise (TTX)	**Add**			A TTX is typically held in an informal setting intended to generate discussion of various issues regarding a hypothetical, simulated emergency. TTXs can be used to enhance general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in attitudes.	FEMA
TLD	**Add**	Acronym		Top-Level Domain	IETF, RFC 1591
TT&E	**Add**	Acronym		Tests, Training, and Exercises	FEMA
TTX	**Add**	Acronym		Tabletop Exercise	FEMA
Tests, Training, and Exercises (TT&E)	**Modify**		Measures to ensure that an organization's Continuity plan is capable of supporting the continued execution of the organization's Essential Functions throughout the duration of a Continuity event. TT&E activities are designed to familiarize, impart skills and ensure viability of Continuity plans.	Activities designed to familiarize, impart skills, and ensure viability of continuity plans. TT&E aids in verifying that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity plan activation.	FEMA
Threat	**Modify**		An intentional or accidental action, activity or event that can adversely impact agency information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	NIST
Top-Level Domain	**Add**			In the Domain Name System (DNS) naming of computers there is a hierarchy of names. The root of system is unnamed. There are a set of what are called "top-level domain names" (TLDs). These are the generic TLDs (.EDU, .COM, .NET, .ORG, .GOV, .MIL, and .INT), and the two letter country codes (e.g. .US, .CA, .EU, etc.) from ISO-3166.	IETF, RFC 1591
Vendor	**Add**			A commercial supplier of software, hardware, services and/or information.	NIST